

DVORETZKY'S THEOREM AND THE COMPLEXITY OF ENTANGLEMENT DETECTION

GUILLAUME AUBRUN AND STANISŁAW J. SZAREK

ABSTRACT. The well-known Horodecki criterion asserts that a state ρ on $\mathbb{C}^d \otimes \mathbb{C}^d$ is entangled if and only if there exists a positive map $\Phi : \mathbf{M}_d \rightarrow \mathbf{M}_d$ such that the operator $(\Phi \otimes \text{Id})(\rho)$ is not positive semi-definite. We show that the number of such maps needed to detect all the robustly entangled states (i.e., states ρ which remain entangled even in the presence of substantial randomizing noise) exceeds $\exp(cd^3 / \log d)$. The proof is based on the 1977 inequality of Figiel–Lindenstrauss–Milman, which ultimately relies on Dvoretzky's theorem about almost spherical sections of convex bodies. We interpret that inequality as a statement about approximability of convex bodies by polytopes with few vertices or with few faces and apply it to the study of fine properties of the set of quantum states and that of separable states. Our results can be thought of as geometrical manifestations of the complexity of entanglement detection.

INTRODUCTION

Entanglement [12, 35, 42] lies at the heart of quantum mechanics and is a fundamental resource for quantum information and computation. It underlies many of the most striking potential applications of quantum phenomena to information processing such as, for example, teleportation [8]. However, its properties remain elusive; even at the mathematical level, the current understanding of entanglement in high-dimensional systems remains very incomplete, and not for the lack of trying. In particular, there is an extensive literature on the entanglement detection, of which we mention below just several highlights.

It is an elementary observation that if ρ is a separable state on $\mathbb{C}^d \otimes \mathbb{C}^d$ and $\Phi : \mathbf{M}_d \rightarrow \mathbf{M}_d$ is a positive map (i.e., a map which preserves positive semi-definiteness of $d \times d$ matrices), then $(\Phi \otimes \text{Id})(\rho)$ is positive semi-definite. A remarkable result known as the Horodecki criterion [24] asserts that the converse is true: if a state ρ on $\mathbb{C}^d \otimes \mathbb{C}^d$ is entangled, then there exists a positive map $\Phi : \mathbf{M}_d \rightarrow \mathbf{M}_d$ which detects its entanglement in the sense that $(\Phi \otimes \text{Id})(\rho)$ has a negative eigenvalue. Such a map is called an *entanglement witness*.

Key words and phrases. Complexity of entanglement, Figiel–Lindenstrauss–Milman inequality, Dvoretzky's theorem, Facial dimension, Verticil dimension.

The authors thank the Instituto de Ciencias Matemáticas in Madrid where this work was initiated. The research of GA was supported in part by Agence Nationale de la Recherche (France) grants OSQPI (2011-BS01-008-02) and StoQ (2014-CE25-0003). The research of SJS was supported in part by grants from the National Science Foundation (U.S.A.) and by the first ANR grant listed above.

The study of positive maps between matrix algebras is notoriously difficult. The situation is quite simple when $d = 2$: any positive map on M_2 is decomposable [37], i.e., can be written as $\Phi_1 + \Phi_2 \circ T$ where Φ_1, Φ_2 are completely positive maps and T is the transposition on M_2 . (Of course completely positive maps by themselves are useless for the task of entanglement detection since all their extensions are positive by definition.) It follows that the well-known Peres partial transposition criterion is a necessary and sufficient condition for separability of 2-qubits states [30, 24].

The situation in higher dimensions is much less clear. To describe it, we will use the following concept. Let $\mathcal{F} = (\Phi_i)$ be a family of positive maps on M_d and let E be a subset of the set of entangled states on $\mathbb{C}^d \otimes \mathbb{C}^d$. We say that \mathcal{F} is *universal* for E if for every $\rho \in E$, there is an index i such that Φ_i is an entanglement witness for ρ , i.e., $(\Phi_i \otimes \text{Id})(\rho)$ has a negative eigenvalue.

First, for $d \geq 3$, the partial transposition criterion is no longer sufficient [25]. Moreover, for such d , any family \mathcal{F} which is universal for all entangled states must be infinite (this result is announced in [36] and based on [19]).

However, asking for detecting *all* entangled states is probably too demanding for any practical purpose. We say that a state ρ on $\mathbb{C}^d \otimes \mathbb{C}^d$ is *robustly entangled* if $\frac{1}{2}(\rho + \rho_*)$ is entangled, where $\rho_* = I/d^2$ denotes the maximally mixed state. In other words, robustly entangled states remain entangled even in the presence of substantial randomizing noise. The main result of the paper is a super-exponential lower bound on the cardinality of any universal family which detects robust entanglement.

Theorem 1. *There is a universal constant $c > 0$ such that the following holds. Consider $d \geq 2$ and let $(\Phi_i)_{1 \leq i \leq N}$ be a family of positive maps on M_d which is universal for all robustly entangled states. Then $N + 1 \geq \exp(cd^3 / \log d)$.*

We used the factor $\frac{1}{2}$ in the definition of robust entanglement only for simplicity; the same proof works for any fixed choice of weights. With a little care, the argument gives actually much more.

Theorem 1'. *There are universal constants $c_0, c > 0$ such that the following holds. Consider $d \geq 2$ and set $\varepsilon_d = c_0 \log d / \sqrt{d}$. Let $(\Phi_i)_{1 \leq i \leq N}$ be a family of positive maps on M_d which is universal for the set*

$$(1) \quad \{\rho \text{ state on } \mathbb{C}^d \otimes \mathbb{C}^d : \varepsilon_d \rho + (1 - \varepsilon_d) \rho_* \text{ is entangled}\}.$$

Then $N + 1 \geq \exp(cd^2 \log d)$.

The fact that universal families must be large is not surprising. Indeed, each positive map leads to a test for entanglement detection which runs in polynomial time. Consequently, the existence of small universal families would have to be reconciled with the known result that deciding whether a given state is separable or entangled is an NP-hard problem. This was first observed by Gurvits [16] and refined in [26, 14]; other relevant references include [9, 20, 18]. However, to the best of our knowledge, results in the spirit of Theorem 1 cannot be derived from the existing literature. For starters, the

complexity results cited above that address lower bounds generally focus on states situated *very* close to the separability/entanglement border (which precludes the robustness feature present in our setting) or are based on computational assumptions such as in [20]. An exception is the forthcoming work [21], which addresses lower bounds on the size of some relaxations of entanglement detection problems. Let us also mention a result from [39] that is similar in spirit: the set of completely positive maps occupies a subexponentially (in the dimension of that set) small proportion, in terms of volume, of the set of all positive maps.

Our proof of Theorem 1 is geometric and is based on the following observation due to Figiel–Lindenstrauss–Milman [13]: an n -dimensional polytope which admits a center of symmetry cannot have few faces and – simultaneously – few vertices. Complexity must lie somewhere. This paradigm is actually rather general and can be applied to the set of separable states (although it is neither a polytope nor centrally symmetric): given that it has “few” extreme points, it must have many “faces.” Since we can upper-bound the number of faces provided by each test detecting entanglement, we conclude that many tests are needed. This vague scheme can be converted to a rigorous proof through the introduction of the *verticial dimension* and the *facial dimension* of a convex body K , which quantify the number of vertices (resp., faces) required for a polytope to approximate K within a constant factor, and are measures of algorithmic complexity of K .

The paper is organized as follows. The remainder of the Introduction is devoted to the notation and basic background results. Section 1 introduces the concepts of verticial and facial dimensions, and states the fundamental Figiel–Lindenstrauss–Milman inequality (6) asserting that their product must be large. That inequality is subsequently related to the classical Dvoretzky–Milman theorem in Section 2. Section 3 estimates these parameters for the sets of all states and that of separable states (sometimes proved up to a logarithmic factor, which is irrelevant for the main argument). Section 4 applies these concepts and estimates to derive Theorems 1 and 1'. Finally, in Section 5 we prove the full strength of the bounds on verticial dimensions stated in Section 3 by removing the “technical” logarithmic factor. The bounds (10) and (11) are surprisingly subtle and the arguments leading to them are of independent interest.

The results from this paper will be incorporated in a forthcoming book [2], which contains more background on both Quantum Information Theory and Asymptotic Geometric Analysis, and many examples of their interaction.

Notation and basic facts. A convex body $K \subset \mathbb{R}^n$ is an n -dimensional convex compact set. Denote by $|\cdot|$ the Euclidean norm in \mathbb{R}^n or \mathbb{C}^n , and by B_2^n and S^{n-1} the unit ball and unit sphere in \mathbb{R}^n . A ε -net in a set $S \subset \mathbb{R}^n$ is a subset $\mathcal{N} \subset S$ with the property that for any $x \in S$ there is $y \in \mathcal{N}$ with $|x - y| \leq \varepsilon$. We will repeatedly use the following elementary bound.

Lemma 2. *For every $\varepsilon \in (0, 1)$ and $n \in \mathbb{N}$, there is an ε -net \mathcal{N} in S^{n-1} with $\text{card } \mathcal{N} \leq (1 + 2/\varepsilon)^n$. Conversely, if \mathcal{N} is a ε -net in S^{n-1} for some $\varepsilon \in (0, \sqrt{2})$, then $\text{card } \mathcal{N} \geq 2/\sin^{n-1} \theta$, where $\theta = 2 \arcsin(\varepsilon/2) < \pi/2$ is the angle between two points in S^{n-1} which are ε -distant.*

The first part of Lemma 2 is proved by a volumetric argument (see [31], Lemma 4.10). The second part follows from the fact that the proportion of S^{n-1} covered by a spherical cap of angular radius θ is less than $\frac{1}{2}(\sin \theta)^{n-1}$, as can be checked by simple geometric considerations.

The unit sphere in \mathbb{C}^m is denoted $S_{\mathbb{C}^m}$. Since $S_{\mathbb{C}^m}$ identifies with S^{2m-1} as a metric space, the results from Lemma 2 also apply. We denote by \mathbf{M}_m the algebra of complex $m \times m$ matrices, which we identify with operators on \mathbb{C}^m . We use Dirac bra-ket notation. In particular, if $\psi \in S_{\mathbb{C}^m}$, then $|\psi\rangle\langle\psi|$ denotes the rank 1 orthogonal projection onto $\mathbb{C}\psi$. The inner product of vectors ψ, φ is denoted $\langle\psi|\varphi\rangle$, and if $A \in \mathbf{M}_m$ we write $\langle\psi|A|\varphi\rangle$ for $\langle\psi|A(\varphi)\rangle$. Such notation leads to visually pleasant formulas such as $\text{Tr}(|\psi\rangle\langle\psi|A) = \langle\psi|A|\psi\rangle$. A fundamental object, which we denote by $\mathbf{D}(\mathbb{C}^m)$ or simply by \mathbf{D} when the context is clear, is the set of (mixed) states on \mathbb{C}^m defined as

$$\mathbf{D}(\mathbb{C}^m) := \{\rho \in \mathbf{M}_m : \rho = \rho^\dagger, \rho \geq 0, \text{Tr } \rho = 1\} = \text{conv}\{|\psi\rangle\langle\psi| : \psi \in S_{\mathbb{C}^m}\}.$$

States of the form $|\psi\rangle\langle\psi|$ are called pure states and coincide with the set of extreme points of \mathbf{D} . We call maximally mixed state the state $\rho_* := \mathbf{I}/m$, where \mathbf{I} is the identity matrix. When \mathbb{C}^m is identified with the tensor product $\mathbb{C}^d \otimes \mathbb{C}^d$ (with $m = d^2$), we denote by $\text{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)$, or simply Sep , the subset of \mathbf{D} formed by separable states:

$$\text{Sep} := \text{conv}\{|\psi \otimes \varphi\rangle\langle\psi \otimes \varphi| : \psi, \varphi \in S_{\mathbb{C}^d}\}.$$

States which are not separable are called entangled. Both \mathbf{D} and Sep live in the affine space

$$(2) \quad H = \{A \in \mathbf{M}_m : A = A^\dagger, \text{Tr } A = 1\}.$$

In order to use tools from geometry of normed spaces (a.k.a. *asymptotic geometric analysis*), we consider H as a vector space whose origin is the maximally mixed state $\rho_* = \mathbf{I}/m$. We use \bullet to denote scalar multiplication in H when interpreted as a vector space, i.e., for $\rho \in H$ and $t \in \mathbb{R}$,

$$(3) \quad t \bullet \rho := t\rho + (1-t)\rho_*.$$

If $K \subset H$, then denote $t \bullet K = \{t \bullet x : x \in K\}$. We repeatedly use the following fact: for convex bodies K, L in H and $t \geq 0$, the inclusion $t \bullet K \subset L$ is equivalent to fact that the inequality

$$t \sup_{\rho \in K} \text{Tr}(A\rho) \leq \sup_{\rho \in L} \text{Tr}(A\rho)$$

holds for every trace zero Hermitian matrix A .

We equip H with the Hilbert–Schmidt (or Frobenius) norm $\|A\|_{\text{HS}} = (\text{Tr } A^2)^{1/2}$, so that the unit ball is $B_{\text{HS}} := \{A \in H : \|A - \rho_*\|_{\text{HS}} \leq 1\}$. Denote also by $\|\cdot\|_{\text{op}}$ the operator norm and by $\|A\|_{\text{Tr}} = \text{Tr}((AA^\dagger)^{1/2})$ the trace-class norm.

1. VERTICIAL AND FACIAL DIMENSION OF CONVEX SETS

Let $K \subset \mathbb{R}^n$ be a convex body containing 0 in the interior. All polytopes we consider are convex. Fix a number $A > 1$, our resolution parameter. Define the *vertical dimension* of K as

$\dim_V(K, A) := \log \inf\{N : \text{there is a polytope } P \text{ with } N \text{ vertices s.t. } K \subset P \subset AK\}$
and the *facial dimension* of K as

$\dim_F(K, A) := \log \inf\{N : \text{there is a polytope } Q \text{ with } N \text{ facets s.t. } K \subset Q \subset AK\}$,

where by facets we mean faces of dimension $n-1$. We set the resolution parameter A as a default value equal to 4 and write $\dim_V(K) := \dim_V(K, 4)$ and $\dim_F(K) := \dim_F(K, 4)$. All the results below are only affected in the values of the numerical constants (implicit in the notation $O(\cdot)$, $\Theta(\cdot)$ and $\Omega(\cdot)$) if 4 is replaced by another number larger than 1. However, the character of the dependence on A will be important in some applications.

We note that these concepts are linear invariants in the following sense: $\dim_V(TK) = \dim_V(K)$ and $\dim_F(TK) = \dim_F(K)$ for any $T \in \text{GL}_n$. Moreover, there are dual to each other: if we define the *polar* of a convex body $K \subset \mathbb{R}^n$ (say, containing 0 in the interior) as the convex body

$$K^\circ = \{x \in \mathbb{R}^n : \langle x, y \rangle \leq 1 \text{ for all } y \in K\},$$

then $\dim_V(K^\circ) = \dim_F(K)$ and $\dim_F(K^\circ) = \dim_V(K)$. Indeed, P is a polytope with N facets if and only if P° is a polytope with N vertices.

We also note that if $E \subset \mathbb{R}^n$ is a linear subspace, $\dim_F(K \cap E) \leq \dim_F K$ and $\dim_V(P_E K) \leq \dim_V K$ where P_E denotes the orthogonal projection onto E . These inequalities follow from the fact that projections do not increase the number of vertices of polytopes, while sections do not increase the number of facets.

For any convex body $K \subset \mathbb{R}^n$ which is 0-symmetric (i.e., such that $K = -K$), we have $\dim_V(K) = O(n)$ and $\dim_F(K) = O(n)$ by a standard volumetric argument (see, e.g., Lemma 1 in [1]). This fails in complete generality without the symmetry assumption, but for wrong reasons: consider the case of a disk in \mathbb{R}^2 which contains the origin *very* close to its boundary. If we insist that, for example, K has centroid at the origin, then the inequalities $\dim_V(K) = O(n)$ and $\dim_F(K) = O(n)$ still hold, but this is less obvious than in the symmetric case (see [10, 7, 28, 38, 2] for this and related questions).

Define also the *asphericity* of a convex body $K \subset \mathbb{R}^n$ as

$$(4) \quad a(K) = \inf \left\{ \frac{R}{r} : \text{there is a 0-symmetric ellipsoid } \mathcal{E} \text{ with } r\mathcal{E} \subset K \subset R\mathcal{E} \right\}.$$

The reader will notice that, arguably, it would be more natural and more functorially sound to define $\dim_F(\cdot)$, $\dim_V(\cdot)$ and $a(\cdot)$ with an additional infimum over all translates of K : we would end up then with *affine* invariants (and not just *linear* invariants). However, this is not necessary in our setting and would in fact lead to complications in duality considerations.

We will use in a fundamental way the following result, which appears only implicitly (see the paragraphs preceding Example 3.5) in [13]. We also make explicit the dependence on resolution parameters.

Theorem 3. *For any convex body $K \subset \mathbb{R}^n$ containing the origin in the interior we have*

$$(5) \quad \dim_F(K) \dim_V(K) a(K)^2 = \Omega(n^2).$$

More generally, if $A, B > 1$, then

$$(6) \quad A^2 \dim_F(K, A) \cdot B^2 \dim_V(K, B) \cdot a(K)^2 = \Omega(n^2).$$

Theorem 3 is fairly sharp for many convex bodies, as is illustrated in Table 1 below. Moreover, for all those examples it is enough to consider in (4) Euclidean balls rather than general ellipsoids \mathcal{E} .

	dimension	$a(K)$	$\dim_V(K)$	$\dim_F(K)$
Euclidean ball B_2^n	n	1	$\Theta(n)$	$\Theta(n)$
Cube $[-1, 1]^n$	n	\sqrt{n}	$\Theta(n)$	$\Theta(\log n)$
Simplex in \mathbb{R}^n	n	n	$\Theta(\log n)$	$\Theta(\log n)$
Set of states on \mathbb{C}^m	$m^2 - 1$	$m - 1$	$\Theta(m)$	$\Theta(m)$
Set of separable states on $\mathbb{C}^d \otimes \mathbb{C}^d$	$d^4 - 1$	$d^2 - 1$	$\Theta(d \log d)$	$\Omega(d^3 / \log d)$

TABLE 1. Parameters appearing in (5) for some families of convex bodies.

Let us give references/justifications for the values appearing in the table. First, consider the case of the Euclidean ball, which is simple but fundamental. Again, we also make explicit the dependence on resolution parameters

Lemma 4. *For $n \geq 1$ and $A > 1$, we have $\dim_V(B_2^n, A) = \dim_F(B_2^n, A) \geq \frac{n-1}{2A^2}$.*

Proof. First, since $(B_2^n)^\circ = B_2^n$, the vertical and facial dimensions coincide; this justifies the equality in the assertion. Now assume that $\dim_V(B_2^n, A) = \log N$, so that there exists a polytope P with N vertices such that $A^{-1}B_2^n \subset P \subset B_2^n$. Next, define the volume radius of P as the quantity $\text{vrad}(P) := (\text{vol } P / \text{vol } B_2^n)^{1/n}$. Our assumptions on P imply then that $\text{vrad}(P) \geq A^{-1}$. This has to be compared with the following general upper bound (valid for $n \geq 2$, which we may clearly assume): if $Q \subset B_2^n$ is a polytope

with N vertices, then $\text{vrad}(Q) \leq \sqrt{\frac{2 \log N}{n-1}}$ (see, e.g., [2] or [4]). Combining these two inequalities yields $A^{-1} \leq \sqrt{\frac{2 \log N}{n-1}}$, which is an equivalent form of the inequality in the assertion. \square

The estimates for the cube and for the simplex are easy to prove and are not used in this paper. For the simplex, we assume the center of mass to be at the origin. In particular, if we think of the n -dimensional simplex as the set of classical states (i.e., probability measures) on $n+1$ points, the role of the origin is played by the uniform probability measure $(\frac{1}{n+1}, \dots, \frac{1}{n+1})$. This is analogous to the quantum case, where the maximally mixed state ρ_* is considered as the origin.

Next, let us consider $D = D(\mathbb{C}^m)$, the set of states on \mathbb{C}^m . It is elementary to check that

$$(7) \quad \frac{1}{\sqrt{m(m-1)}} \bullet B_{\text{HS}} \subset D \subset \sqrt{\frac{m-1}{m}} \bullet B_{\text{HS}}$$

so that $a(D) \leq m-1$. We have actually $a(D) = m-1$: by a symmetry argument, the optimal ellipsoid must be a multiple of the Hilbert–Schmidt ball, and the values in (7) are optimal. The self-duality of the cone of positive semi-definite matrices implies that

$$(8) \quad D^\circ = (-m) \bullet D$$

(polarity in H , with ρ_* as the origin), so that $\dim_F(D) = \dim_V(D)$. The $\Theta(m)$ estimate appears in Theorem 6.

Finally, if Sep is the set of separable states on $\mathbb{C}^d \otimes \mathbb{C}^d$, then

$$(9) \quad \frac{1}{\sqrt{d^2(d^2-1)}} \bullet B_{\text{HS}} \subset \text{Sep} \subset \sqrt{\frac{d^2-1}{d^2}} \bullet B_{\text{HS}}.$$

While the second inclusion in (9) is elementary, the first one is a non-trivial result due to Gurvits and Barnum [17]. It follows that $a(\text{Sep}) \leq d^2-1$ and, like for D , there is actually an equality. The vertical dimension of Sep is computed in Theorem 7 and the lower bound on the facial dimension follows then from Theorem 3. This is reminiscent of the arguments from [5, 6], where calculating *directly* certain invariants of the set Sep was not feasible because of the hardness of detecting entanglement, but it was possible to reasonably estimate the values of those invariants using duality considerations and deep results from asymptotic geometric analysis.

2. CONNEXION WITH DVORETZKY'S THEOREM

Theorem 3 is actually a consequence of the Milman's version of Dvoretzky's theorem [11, 29], which gives a sharp formula for the dimension of almost spherical sections of convex bodies. Recall that to each convex body $K \subset \mathbb{R}^n$ containing the origin in the interior, we may associate its gauge defined for $x \in \mathbb{R}^n$ as

$$\|x\|_K := \inf\{t \geq 0 : x \in tK\}.$$

This gauge is a norm if and only if K is symmetric.

Theorem 5 (Dvoretzky–Milman theorem). *There is an absolute constant $c > 0$ such that the following holds. Let K be a convex body in \mathbb{R}^n such that $rB_2^n \subset K$ for some $r > 0$, and let $\varepsilon \in (0, 1)$. Denote by M the expectation of $\|X\|_K$ where X is a uniformly distributed random vector on S^{n-1} . Then there exist an integer $k \geq c\varepsilon^2 M^2 r^2 n$ and a k -dimensional subspace $E \subset \mathbb{R}^n$ such that*

$$(1 - \varepsilon)MB_2^E \subset K \cap E \subset (1 + \varepsilon)MB_2^E$$

where $B_2^E := B_2^n \cap E$ denotes the unit ball in E .

Theorem 5 is a fundamental result in the geometry of high-dimensional convex bodies. If we do not insist on having the correct dependence on ε (which was shown in [15, 34], but which is not needed here), its proof essentially amounts to using concentration of measure in the form of Lévy’s lemma [27], combined with a simple union bound argument. We also note that the hypothesis that K is symmetric present in [29] is not needed in the argument. Another important point is that the conclusion of Theorem 5 holds for most subspaces E , but this aspect is not relevant to the present paper. An application of (the complex version of) Theorem 5 in Quantum Information Theory appears in [3], where it is shown to imply and conceptually simplify Hastings’ result [22] about non-additivity of classical capacity of quantum channels.

For reader’s convenience, and because the statement is only implicit in [13], we reproduce the argument allowing to derive Theorem 3 from Theorem 5. Let K be a convex body in \mathbb{R}^n containing 0 in the interior. Since the vertical and facial dimension are invariant under linear transformations, we may assume that the ellipsoid witnessing the infimum in (4) is a Euclidean ball, i.e., that $rB_2^n \subset K \subset RB_2^n$ with $R/r = a(K)$. Let $M = \mathbf{E} \|X\|_K$ and $M^* = \mathbf{E} \|X\|_{K^\circ}$ where X is a random vector uniformly distributed on the unit sphere. The pointwise inequality $\|\cdot\|_K^{1/2} \|\cdot\|_{K^\circ}^{1/2} \geq 1$ implies by Cauchy–Schwarz inequality that $MM^* \geq 1$.

We apply Theorem 5 to K with $\varepsilon = 1/2$ (say). This yields a subspace $E \subset \mathbb{R}^n$ of dimension $\Omega((rM)^2 n)$ such that

$$\frac{M}{2}B_2^E \subset K \cap E \subset \frac{3M}{2}B_2^E.$$

It follows that $\dim_F(K \cap E, A) \geq \dim_F(B_2^E, 3A) \geq \frac{1}{18A^2}(\dim E - 1)$, where the second inequality comes from Lemma 4. Consequently

$$\dim_F(K, A) \geq \dim_F(K \cap E, A) = \Omega((rM)^2 n A^{-2}).$$

We apply the same argument to K° (note that $R^{-1}B_2^n \subset K^\circ$) and obtain that $\dim_F(K^\circ, B) = \Omega((M^*/R)^2 n B^{-2})$. Since $\dim_V(K, B) = \dim_F(K^\circ, B)$, it follows that

$$\dim_F(K, B) \dim_V(K, A) = \Omega(n^2 (MM^*)^2 (r/R)^2 A^{-2} B^{-2}) = \Omega(n^2 A^{-2} B^{-2} / a(K)^2),$$

as needed.

3. FACIAL AND VERTICIAL DIMENSION OF D AND Sep

In this section we denote $D = D(\mathbb{C}^m)$ and $\text{Sep} = \text{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)$. We recall that the role of the origin is played by the maximally mixed state, i.e., that the condition on polytopes appearing in the definition of $\dim_V(D)$ or $\dim_F(D)$ is $P \subset D \subset 4 \bullet P$, and similarly for Sep . In order to justify all the estimates appearing in Table 1, we need to prove the following two theorems.

Theorem 6. *Let $D = D(\mathbb{C}^m)$. We have*

$$(10) \quad d_F(D) = d_V(D) = \Theta(m).$$

Theorem 7. *Let $\text{Sep} = \text{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)$. We have*

$$(11) \quad \dim_V(\text{Sep}) = \Theta(d \log d)$$

and

$$(12) \quad \dim_F(\text{Sep}) = \Omega(d^3 / \log d).$$

More generally, for any $A > 1$,

$$(13) \quad \dim_F(\text{Sep}, A) = \Omega(d^3 A^{-2} / \log d).$$

As we already noted, the self-duality of D (see (8)) implies that $\dim_V(D) = \dim_F(D)$. Since $a(D) = m - 1$, Theorem 3 implies that

$$d_F(D) = d_V(D) = \Omega(m).$$

It is also easy to supply a direct argument going along the same lines as (but simpler than) the proof of the lower bound in (11) presented later in this Section.

Surprisingly, that the upper bound $d_V(D) = O(m)$ is not that easy to establish and so we postpone the argument to Section 5. However, the simpler bound $O(m \log m)$, which suffices for the proof of Theorem 1, follows immediately from the following elementary observation combined with Lemma 2 (both applied with $\delta = \frac{3}{8m}$).

Lemma 8. *Let \mathcal{M} be a δ -net in $(S_{\mathbb{C}^m}, |\cdot|)$. Then*

$$(14) \quad (1 - 2m\delta) \bullet D \subset \text{conv}\{|\psi_i\rangle\langle\psi_i| : \psi_i \in \mathcal{M}\} \subset D.$$

The reader will notice that the proof given below can be fine-tuned to yield a slightly better – but more complicated – factor $(1 - 2(m - 1)\delta)$ in (14).

Proof. We have to show that, for any trace zero Hermitian matrix A ,

$$\lambda_1(A) := \sup_{\psi \in S_{\mathbb{C}^m}} \langle \psi | A | \psi \rangle \leq (1 - 2\delta m)^{-1} \sup_{\psi_i \in \mathcal{M}} \langle \psi_i | A | \psi_i \rangle.$$

Since A has trace 0, we have $\|A\|_{\text{op}} \leq m\lambda_1(A)$. Given $\psi \in S_{\mathbb{C}^m}$, there is $\psi_i \in \mathcal{M}$ with $|\psi - \psi_i| \leq \delta$. By the triangle inequality, we have

$$(15) \quad \langle \psi | A | \psi \rangle \leq \delta \|A\|_{\text{op}} + \langle \psi | A | \psi_i \rangle$$

$$(16) \quad \leq 2\delta \|A\|_{\text{op}} + \langle \psi_i | A | \psi_i \rangle$$

$$(17) \quad \leq 2\delta m\lambda_1(A) + \langle \psi_i | A | \psi_i \rangle.$$

Taking supremum over ψ , we get $\lambda_1(A) \leq 2\delta m\lambda_1(A) + \sup\{\langle \psi_i | A | \psi_i \rangle : \psi_i \in \mathcal{M}\}$ and the result follows. \square

We now prove Theorem 7. We first note that since $a(\text{Sep}) = d^2 - 1$, once we know that (11) holds, (12) and (13) follow by an application of Theorem 3. It is likely that the lower bound (12) on $\dim_F(\text{Sep})$ is not sharp; any improvement would reflect on the estimate in Theorem 1.

Proof of the upper bound in (11). Let \mathcal{N} be a ε -net in $(S_{\mathbb{C}^d}, |\cdot|)$ with ε to be determined. We want to show that

$$(18) \quad \frac{1}{4} \bullet \text{Sep} \subset \text{conv} \{ |\psi_i \otimes \psi_j\rangle \langle \psi_i \otimes \psi_j| : \psi_i, \psi_j \in \mathcal{N} \} \subset \text{Sep}.$$

Equivalently, we have to show that for any trace zero Hermitian matrix A we have

$$W := \sup_{\psi, \varphi \in S_{\mathbb{C}^d}} \langle \psi \otimes \varphi | A | \psi \otimes \varphi \rangle \leq 4 \sup_{\psi_i, \psi_j \in \mathcal{N}} \langle \psi_i \otimes \psi_j | A | \psi_i \otimes \psi_j \rangle.$$

First, note that using the left inclusion from (9), it follows that

$$W \geq \frac{1}{d^2} \|A\|_{\text{HS}} \geq \frac{1}{d^2} \|A\|_{\text{op}}.$$

Given $\varphi, \psi \in S_{\mathbb{C}^d}$, there are $\psi_i, \psi_j \in \mathcal{N}$ with $|\varphi - \psi_i| \leq \varepsilon$ and $|\psi - \psi_j| \leq \varepsilon$. Using the triangle inequality as in (15)-(16), we have

$$\langle \varphi \otimes \psi | A | \varphi \otimes \psi \rangle \leq 4\varepsilon \|A\|_{\text{op}} + \langle \psi_i \otimes \psi_j | A | \psi_i \otimes \psi_j \rangle \leq 4\varepsilon d^2 W + \langle \psi_i \otimes \psi_j | A | \psi_i \otimes \psi_j \rangle.$$

Taking supremum over φ, ψ , we obtain

$$W \leq 4\varepsilon d^2 W + \sup_{\psi_i, \psi_j \in \mathcal{N}} \langle \psi_i \otimes \psi_j | A | \psi_i \otimes \psi_j \rangle.$$

We now set $\varepsilon = 3/16d^2$; this guarantees that (18) holds. By Lemma 2, we may choose \mathcal{N} such that $\text{card} \mathcal{N} \leq (16d^2)^{2d}$. Since we produced a polytope P with $(\text{card} \mathcal{N})^2$ vertices such that $\frac{1}{4} \bullet P \subset \text{Sep} \subset P$, it follows that $\dim_V(\text{Sep}) = O(d \log d)$. \square

The estimates used in the argument above may appear quite crude and so it comes as a surprise that the obtained bound is actually tight.

Proof of the lower bound in (11). Let P a polytope with N vertices such that $\frac{1}{4} \bullet \text{Sep} \subset P \subset \text{Sep}$. By Carathéodory's theorem, we may write each vertex of P as a combination of d^4 extreme points of Sep (which are pure product states, i.e., of the form $|\psi \otimes \varphi\rangle \langle \psi \otimes \varphi|$ for unit vectors $\psi, \varphi \in \mathbb{C}^d$). We obtain therefore a polytope Q which is the convex hull

of $N' \leq Nd^4$ pure product states, and such that $\frac{1}{4} \bullet \text{Sep} \subset P \subset Q \subset \text{Sep}$. Let $(|\psi_i \otimes \varphi_i\rangle\langle\psi_i \otimes \varphi_i|)_{1 \leq i \leq N'}$ be the vertices of Q . Fix $\chi \in S_{\mathbb{C}^d}$ arbitrarily. For any $\varphi \in S_{\mathbb{C}^d}$, let $\alpha = \max\{|\langle\varphi|\varphi_i\rangle|^2 : 1 \leq i \leq N'\}$. Consider the linear form

$$g(\rho) = \text{Tr} [\rho (|\chi\rangle\langle\chi| \otimes (\alpha \text{I}_{\mathbb{C}^d} - |\varphi\rangle\langle\varphi|))].$$

For any $1 \leq i \leq N'$ we have

$$g(|\psi_i \otimes \varphi_i\rangle\langle\psi_i \otimes \varphi_i|) = |\langle\chi|\psi_i\rangle|^2(\alpha - |\langle\varphi|\varphi_i\rangle|^2) \geq 0$$

and therefore g is nonnegative on Q . Since $Q \supset \frac{1}{4} \bullet \text{Sep}$, we have

$$\begin{aligned} 0 \leq g\left(\frac{1}{4} \bullet |\chi \otimes \varphi\rangle\langle\chi \otimes \varphi|\right) &= \frac{1}{4} g(|\chi \otimes \varphi\rangle\langle\chi \otimes \varphi|) + \frac{3}{4} g(\rho_*) \\ &= \frac{1}{4}(\alpha - 1) + \frac{3}{4} \times \frac{1}{d} \left(\alpha - \frac{1}{d}\right) \\ &= \frac{1}{4}\alpha \left(1 + \frac{3}{d}\right) - \frac{1}{4} \left(1 + \frac{3}{d^2}\right). \end{aligned}$$

It follows that

$$\alpha \geq \frac{1 + \frac{3}{d^2}}{1 + \frac{3}{d}} \geq 1 - \frac{3}{d}.$$

In other words, we showed that for every $\varphi \in S_{\mathbb{C}^d}$ there is an index $i \in \{1, \dots, N'\}$ such that $|\langle\varphi|\varphi_i\rangle|^2 \geq 1 - 3/d$. This means that $(\varphi_i)_{1 \leq i \leq N'}$ is an $O(1/\sqrt{d})$ -net in the projective space over \mathbb{C}^d , when equipped with the quotient metric from $(S_{\mathbb{C}^d}, |\cdot|)$. It follows that the set

$$\mathcal{N} = \{e^{2i\pi j/d} \varphi_i : 1 \leq i \leq N', 1 \leq j \leq d\}$$

is an $O(1/\sqrt{d})$ -net in $S_{\mathbb{C}^d}$. Thus, by Lemma 2, $\text{card } \mathcal{N} \geq (c\sqrt{d})^{2d-1}$ for some absolute constant $c > 0$. At the same time, $\text{card } \mathcal{N} \leq dN' \leq d^5 N$, and combining the two bounds we infer that $\log N = \Omega(d \log d)$, as asserted. \square

4. EXPONENTIALLY MANY POSITIVE MAPS ARE REQUIRED TO DETECT ROBUST ENTANGLEMENT

In this section we prove Theorems 1 and 1'. In the process, the symbol D will always stand for the set of states on $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^d$ and $\text{Sep} \subset \text{D}$ for the corresponding set of separable states. Next, $B^{\text{sa}} = B^{\text{sa}}(\mathcal{H})$ will denote the space of self-adjoint operators on \mathcal{H} , while $\mathcal{PSD} \subset B^{\text{sa}}$ will be the cone of positive semidefinite operators on \mathcal{H} . Let $\{\Phi_1, \dots, \Phi_N\}$ be a family of N positive maps on M_d which satisfies the hypothesis of Theorem 1 or Theorem 1'. This is equivalent to the right hand side inclusion in

$$(19) \quad \text{Sep} \subset \bigcap_{i=1}^N \{\rho \in \text{D} : (\Phi_i \otimes \text{Id})(\rho) \in \mathcal{PSD}\} \subset A \bullet \text{Sep}.$$

where either $A = 2$ (Theorem 1) or $A = 1/\varepsilon_d = c_0^{-1}\sqrt{d}/\log d$ (Theorem 1'). [The left hand side inclusion is the easy part of the Horodecki criterion.] The value of the (universal positive) constant c_0 will be determined at the end of the proof.

The idea of the argument is to show that each of the sets appearing under the intersection in (19) can be well-approximated by a polytope with “not too many” facets. Since the number of facets of a polytope is subadditive under intersections, we can combine this fact with the estimates ((12) or (13)) on the facial dimension of Sep , which will lead to a lower bound on N .

To that end, we note first that we can assume that $\Phi_i(\mathbf{I})$ is invertible for every i . Indeed, if this is not the case, denote by $E \subsetneq \mathbb{C}^d$ the range of $\Phi_i(\mathbf{I})$ (which is a positive operator) and replace Φ_i by $\tilde{\Phi}_i : X \mapsto \Phi_i(X) + P_{E^\perp}XP_{E^\perp}$. The map $\tilde{\Phi}_i$ is clearly positive and has the property that, for any state ρ on $\mathbb{C}^d \otimes \mathbb{C}^d$, we have

$$(\Phi_i \otimes \text{Id})(\rho) \in \mathcal{PSD} \iff (\tilde{\Phi}_i \otimes \text{Id})(\rho) \in \mathcal{PSD}.$$

(The key point in inferring the latter is that positivity of Φ_i implies then that, for any $X \in \mathbf{M}_d$, the range of $\Phi_i(X)$ is contained in E .) Further, we can also assume that Φ_i is unital (i.e., that $\Phi_i(\mathbf{I}) = \mathbf{I}$) by considering the map $X \mapsto \Phi_i(\mathbf{I})^{-1/2}\Phi_i(X)\Phi_i(\mathbf{I})^{-1/2}$.

We now set $\varepsilon = 1/(1+d)$ and $\delta = \varepsilon/2d^2$, and choose a δ -net \mathcal{N} in $S_{\mathbb{C}^d \otimes \mathbb{C}^d}$. By Lemma 2, we may assume that $\log \text{card } \mathcal{N} = O(d^2 \log d)$. We know from Lemma 8 that $(1-\varepsilon) \bullet D \subset Q \subset D$, where Q is the polytope

$$Q = \text{conv}\{|\psi\rangle\langle\psi| : \psi \in \mathcal{N}\}.$$

It follows from (8) that the polytope $P := (-(1-\varepsilon)d^{-2}) \bullet Q^\circ$, which has at most $\text{card } \mathcal{N}$ facets, satisfies

$$(20) \quad (1-\varepsilon) \bullet D \subset P \subset D.$$

It is now instructive to complete the argument under the additional assumption that each Φ_i is also trace-preserving. Since $\Phi_i \otimes \text{Id}$ is then likewise trace-preserving, the condition $(\Phi_i \otimes \text{Id})(\rho) \in \mathcal{PSD}$ from (19) is equivalent to $\rho \in (\Phi_i \otimes \text{Id})^{-1}(D)$ and so, in view of (20),

$$(\Phi_i \otimes \text{Id})^{-1}(P) \subset \{\rho : (\Phi_i \otimes \text{Id})(\rho) \in \mathcal{PSD}\} \subset (1-\varepsilon)^{-1}(\Phi_i \otimes \text{Id})^{-1}(P).$$

This means that we succeeded in approximating the sets from (19) by polyhedra with $\exp(O(d^2 \log d))$ facets, as required for the heuristics we sketched earlier. Note that the additional constraint $\rho \in D$ can be handled in a formal way by adding to the family $\{\Phi_i\}$ the map $\Phi_0 = \text{Id}$, and that Φ_i being unital translates to $(\Phi_i \otimes \text{Id})(\rho_*) = \rho_*$, which assures that we are \bullet -dilating all sets with respect to the same point.

The general case requires some tweaking: we need to be able to control how far Φ_i and $\Phi_i \otimes \text{Id}$ are from being trace-preserving. We will use the following

Lemma 9. *Let $\Phi : \mathbf{M}_d \rightarrow \mathbf{M}_d$ be a positive unital map. Then, for any $\rho \in D$,*

$$0 \leq \text{Tr}[(\Phi \otimes \text{Id})\rho] \leq d.$$

Proof. Since linear forms achieve their extrema on extreme points of convex compact sets, we may assume that $\rho = |\psi\rangle\langle\psi|$ is pure. Let $\psi = \sum \lambda_i e_i \otimes f_i$ the Schmidt decomposition of ψ . Then, by direct calculation,

$$\mathrm{Tr}[(\Phi \otimes \mathrm{Id})\rho] = \sum_{i=1}^d \lambda_i^2 \mathrm{Tr} \Phi(|e_i\rangle\langle e_i|) \leq d,$$

the last inequality following from $\sum \lambda_i^2 = 1$ and from $\Phi(|e_i\rangle\langle e_i|) \leq \Phi(\mathrm{I}) = \mathrm{I}$. \square

Returning to the proof of the Theorems, we denote the convex bodies appearing in (19) by

$$(21) \quad K_i := \{\rho \in D : (\Phi_i \otimes \mathrm{Id})(\rho) \in \mathcal{PSD}\} = D \cap (\Phi_i \otimes \mathrm{Id})^{-1}(\mathcal{PSD})$$

(note that $\rho_* \in K_i$) and define the polyhedral cones

$$(22) \quad \mathcal{C}_i := \{M \in B^{\mathrm{sa}} : (\Phi_i \otimes \mathrm{Id})(M) \in \mathbb{R}_+ P\}.$$

We now claim that

$$(23) \quad \frac{1}{2} \bullet K_i \subset P \cap \mathcal{C}_i \subset K_i.$$

Before proving the claim, let us first show how it implies the Theorems. Combining (23) and (19) we obtain

$$\frac{1}{2} \bullet \mathrm{Sep} \subset \bigcap_{i=1}^N \left(\frac{1}{2} \bullet K_i \right) \subset \bigcap_{i=1}^N (P \cap \mathcal{C}_i) = P \cap \bigcap_{i=1}^N \mathcal{C}_i \subset \bigcap_{i=1}^N K_i \subset A \bullet \mathrm{Sep}.$$

The polytope $R = P \cap \bigcap_{1 \leq i \leq N} \mathcal{C}_i$ has at most $f := (N+1) \exp(Cd^2 \log d)$ facets (i.e., $N+1$ times the number of facets of P), where C is the constant implicit in the notation $\log \mathrm{card} \mathcal{N} = O(d^2 \log d)$. Consequently, by the definition of the facial dimension, we must have $\log f \geq \dim_F(\mathrm{Sep}, 2A)$ and so

$$\log(N+1) + Cd^2 \log d = \log f \geq \dim_F(\mathrm{Sep}, 2A) \geq cd^3 A^{-2} / \log d,$$

where we used (13), $c > 0$ denoting the corresponding absolute constant. In the case of Theorem 1 ($A = 2$), the conclusion is immediate. In the case of Theorem 1' ($A = c_0^{-1} \sqrt{d} / \log d$), we choose $c_0 = \sqrt{2C}/c$ and conclude that $\log(N+1) \geq Cd^2 \log d$, as asserted.

It remains to prove the claim (23). The second inclusion is immediate from the definitions and from (20). For the first inclusion, it is clearly enough to show that $\frac{1}{2} \bullet K_i \subset \mathcal{C}_i$. To that end, let $\rho \in K_i$ and denote $t = \mathrm{Tr}[(\Phi_i \otimes \mathrm{Id})\rho] \geq 0$. We now consider two cases. First, if $t = 0$, then – since $(\Phi_i \otimes \mathrm{Id})(\rho)$ is a positive operator – we must have $(\Phi_i \otimes \mathrm{Id})(\rho) = 0$. Hence trivially $\rho \in \mathcal{C}_i$ and, *a fortiori*, $\frac{1}{2} \bullet \rho \in \mathcal{C}_i$. If $t > 0$, we note that $t^{-1}(\Phi_i \otimes \mathrm{Id})(\rho) \in D$ and that, by Lemma 9, we have $t \leq d$, and therefore $\frac{t}{1+t} = 1 - \frac{1}{1+t} \leq 1 - \frac{1}{1+d} = 1 - \varepsilon$. It thus follows from (20) that

$$\frac{t}{1+t} \bullet t^{-1}(\Phi_i \otimes \mathrm{Id})(\rho) \in \frac{t}{1+t} \bullet D \subset (1 - \varepsilon) \bullet D \subset P.$$

It remains to notice that

$$\frac{t}{1+t} \bullet t^{-1}(\Phi_i \otimes \text{Id})(\rho) = \frac{(\Phi_i \otimes \text{Id})(\rho) + \rho_*}{1+t} = \frac{2}{1+t}(\Phi_i \otimes \text{Id})\left(\frac{\rho + \rho_*}{2}\right),$$

which means that we showed that $(\Phi_i \otimes \text{Id})\left(\frac{1}{2} \bullet \rho\right) \in \frac{1+t}{2} P$. In particular (cf. (22)), $\frac{1}{2} \bullet \rho \in \mathcal{C}_i$, as needed.

5. PROOF OF THEOREM 6

A proof of the lower bound (actually one proof and a sketch of another proof) was given in Section 3, after the statement of Theorem 7. Concerning the upper bound, it may seem reasonable to expect that choosing \mathcal{N} as a δ -net in $S_{\mathbb{C}^d}$ (for some sufficiently small δ independent of d) and taking the convex hull of the corresponding states would yield a polytope P such that $\frac{1}{4} \bullet D \subset P \subset D$. This idea works for the unit ball for the trace class norm – the “symmetrized” version of D – see Lemma 3 in [4]. What makes the problem intriguing is that this such approach fails for D . Indeed, given δ , for d large enough, a δ -net \mathcal{N} may have the property that for some fixed unit vector ψ , we have $|\langle \varphi_i | \psi \rangle| > 1/\sqrt{d}$ for every $\varphi_i \in \mathcal{N}$. It follows that, for every $\rho \in \text{conv}\{|\varphi_i\rangle\langle\varphi_i|\}$, we have $\langle \psi | \rho | \psi \rangle > 1/d$. However, this inequality fails for $\rho = \rho_*$, which shows that even the maximally mixed state does not belong to the convex hull of the net! Elements of the net may somehow conspire towards the direction ψ .

Yet, this approach can be salvaged if we use a balanced δ -net to avoid such conspiracies. Lemma 8 is not enough to directly imply Theorem 6, but it can be bootstrapped to yield the needed estimate. The idea is to use – instead of an arbitrary net – a family of random points independently and uniformly distributed on the unit sphere, and to show that these points satisfy the conclusion of Theorem 6 with high probability. (The observation that randomly chosen subsets often form very efficient nets goes back at least to Rogers [32, 33].) We actually prove the following, which gives Theorem 6 by specializing to $\varepsilon = 3/4$.

Proposition 10. *For every $\varepsilon \in (0, 1)$, there is a constant $C(\varepsilon)$ such that the following holds: for every dimension $d \geq 2$, there exists a family $\mathcal{N} = (\varphi_i)_{1 \leq i \leq N}$ of unit vectors in \mathbb{C}^d , with $N \leq \exp(C(\varepsilon)d)$, such that*

$$(24) \quad (1 - \varepsilon) \bullet D(\mathbb{C}^d) \subset \text{conv}\{|\varphi_i\rangle\langle\varphi_i| : \varphi_i \in \mathcal{N}\}.$$

Proof of Proposition 10. The conclusion (24) can be equivalently reformulated as follows: for any self-adjoint trace zero matrix A we have

$$(25) \quad \lambda_1(A) = \sup_{\psi \in S_{\mathbb{C}^d}} \langle \psi | A | \psi \rangle \leq \frac{1}{1 - \varepsilon} \sup_{\varphi_i \in \mathcal{N}} \langle \varphi_i | A | \varphi_i \rangle.$$

Let \mathcal{M} be a $\frac{\varepsilon}{4d}$ -net in $S_{\mathbb{C}^d}$ given by Lemma 2. By Lemma 8, we have

$$(26) \quad \sup_{\psi \in S_{\mathbb{C}^d}} \langle \psi | A | \psi \rangle \leq \frac{1}{1 - \varepsilon/2} \sup_{\psi \in \mathcal{M}} \langle \psi | A | \psi \rangle.$$

Set $\theta = \sqrt{\varepsilon/8}$. For $\psi \in S_{\mathbb{C}^d}$, denote by $C(\psi, \theta) \subset S_{\mathbb{C}^d}$ the cap with center ψ and radius θ with respect to the geodesic distance. By symmetry, there is a number α (depending on d and ε) such that

$$(27) \quad \frac{1}{\sigma(C(\psi, \theta))} \int_{C(\psi, \theta)} |\varphi\rangle\langle\varphi| d\sigma(\varphi) = (1 - \alpha) \bullet |\psi\rangle\langle\psi|$$

where σ denotes the uniform probability measure on $S_{\mathbb{C}^d}$. Taking (Hilbert-Schmidt) inner product with $|\psi\rangle\langle\psi|$, we obtain

$$1 - \alpha + \frac{\alpha}{d} = \frac{1}{\sigma(C(\psi, \theta))} \int_{C(\psi, \theta)} |\langle\psi|\varphi\rangle|^2 d\sigma(\varphi) \geq \cos^2 \theta \geq 1 - \theta^2$$

so that

$$(28) \quad \alpha \leq \theta^2 \frac{d}{d-1} \leq \varepsilon/4.$$

Denote $L := \sigma(C(\psi, \theta))^{-1}$ and let $\mathcal{N} = \{\varphi_i : 1 \leq i \leq N\}$ be a family of $N = \lceil 2L^3 \rceil$ independent random vectors uniformly distributed on $S_{\mathbb{C}^d}$. (To not to obscure the argument, we will pretend in what follows that $2L^3$ is an integer and so $N = 2L^3$.) We will rely on the following lemma.

Lemma 11. *Let $B_{\text{op}} = \{\Delta \in \mathbf{M}_d : \|\Delta\|_{\text{op}} \leq 1\}$ be the unit ball for the operator norm. For $\psi \in S_{\mathbb{C}^d}$ and $t \geq 0$, the event*

$$E_{\psi, t} = \{(\varphi_i) : (1 - \alpha) \bullet |\psi\rangle\langle\psi| \in tB_{\text{op}} + \text{conv}\{|\varphi_i\rangle\langle\varphi_i| : 1 \leq i \leq 2L^3\}$$

satisfies

$$1 - \mathbf{P}(E_{\psi, t}) \leq \exp(-L) + 2d \exp(-t^2 L^2/8).$$

We apply Lemma 11 with $t = \varepsilon/8d$. When the event $E_{\psi, t}$ holds, we have

$$(29) \quad (1 - \alpha) \langle\psi|A|\psi\rangle \leq t\|A\|_{\text{Tr}} + \sup_{\varphi_i \in \mathcal{N}} \langle\varphi_i|A|\varphi_i\rangle.$$

If the events $E_{\psi, t}$ hold simultaneously for every $\psi \in \mathcal{M}$, we can conclude from (26) and (29) that

$$(30) \quad (1 - \varepsilon/2)(1 - \alpha)\lambda_1(A) \leq t\|A\|_{\text{Tr}} + \sup_{\varphi_i \in \mathcal{N}} \langle\varphi_i|A|\varphi_i\rangle$$

Since A has trace zero, we have $\|A\|_{\text{Tr}} \leq 2d\lambda_1(A)$, and so (30) combined with (28) implies that

$$(1 - \varepsilon)\lambda_1(A) \leq ((1 - \varepsilon/2)(1 - \alpha) - 2td)\lambda_1(A) \leq \sup_{\varphi_i \in \mathcal{N}} \langle\varphi_i|A|\varphi_i\rangle,$$

yielding (25). The Proposition will follow once we establish that, with positive probability, the events $E_{\psi, t}$ hold simultaneously for all $\psi \in \mathcal{M}$. To that end, we use Lemma

11, the estimate $\text{card } \mathcal{M} \leq (12d/\varepsilon)^{2d}$ from Lemma 2, and the union bound

$$(31) \quad \mathbf{P} \left(\bigcap_{\psi \in \mathcal{M}} E_{\psi,t} \right) \geq 1 - \sum_{\psi \in \mathcal{M}} (1 - \mathbf{P}(E_{\psi,t}))$$

$$(32) \quad \geq 1 - \left(\frac{12d}{\varepsilon} \right)^{2d} (\exp(-L) + 2d \exp(-\varepsilon^2 d^{-2} L^2 / 512)).$$

We know from Lemma 2 that $\exp(c_1(\varepsilon)d) \leq L \leq \exp(C_1(\varepsilon)d)$ for some constants $c_1(\varepsilon), C_1(\varepsilon)$ depending only on ε . It follows that the quantity in (31)-(32) is positive for d large enough (depending on ε), yielding a family of $2L^3 \leq 2 \exp(3C_1(\varepsilon)d)$ vectors satisfying the conclusion of Proposition 10. Small values of d are taken into account by adjusting the constant $C(\varepsilon)$ if necessary. \square

Proof of Lemma 11. Let $M_\psi = \text{card}(\mathcal{N} \cap C(\psi, \theta))$. The random variable M_ψ follows the binomial distribution $B(N, p)$ for $N = 2L^3$ and $p = 1/L$. It follows from Hoeffding's inequality [23] that

$$\mathbf{P} \left(B(N, p) \leq \frac{Np}{2} \right) \leq \exp \left(-\frac{p^2 N}{2} \right).$$

Specialized to our situation, this yields

$$(33) \quad \mathbf{P} (M_\psi \leq L^2) \leq \exp(-L).$$

Moreover, conditionally on the value of M_ψ , the points from $\mathcal{N} \cap C(\psi, \theta)$ have the same distribution as $(\varphi_k)_{1 \leq k \leq M_\psi}$, where (φ_k) are independent and uniformly distributed inside $C(\psi, \theta)$. The random matrices

$$X_k = |\varphi_k\rangle\langle\varphi_k| - \mathbf{E} |\varphi_1\rangle\langle\varphi_1| = |\varphi_k\rangle\langle\varphi_k| - (1 - \alpha) \bullet |\psi\rangle\langle\psi|$$

(cf. (27)) are independent mean zero matrices. We now use the matrix Hoeffding inequality (see, e.g., Theorem 1.3 in [40]) to conclude that, for any $t \geq 0$,

$$(34) \quad \mathbf{P} \left(\left\| \frac{1}{M_\psi} \sum_{k=1}^{M_\psi} X_k \right\|_{\text{op}} \geq t \right) \leq 2d \exp(-M_\psi t^2 / 8)$$

(the factor 2 appears because we want to control the operator norm rather than the largest eigenvalue). Define a random matrix Δ by the relation

$$\frac{1}{M_\psi} \sum_{k=1}^{M_\psi} |\varphi_k\rangle\langle\varphi_k| + \Delta = (1 - \alpha) \bullet |\psi\rangle\langle\psi|.$$

The bound (34) translates then into $\mathbf{P}(\|\Delta\|_{\text{op}} \geq t) \leq 2d \exp(-M_\psi t^2 / 8)$. If we remove the conditioning on M_ψ and take (33) into account, we are led to

$$\mathbf{P}(\|\Delta\|_{\text{op}} \geq t) \leq \exp(-L) + 2d \exp(-L^2 t^2 / 8),$$

whence Lemma 11 follows. \square

CONCLUSIONS

As a consequence of Milman's tangible version of Dvoretzky's theorem, we gave an illustration of the complexity of entanglement in high dimensions by showing that the set of separable states requires a super-exponential number of entanglement witnesses to be approximated within a constant factor, independent of the dimension of the instance. To the best of our knowledge, this is the first (unconditional) result of this nature that doesn't collapse in presence of substantial randomizing noise.

There are several possible directions in which this work can be continued.

- **Upper bounds.** Are there matching upper bounds on the cardinal of minimal universal families of positive maps, in the sense of Theorem 1? One upper bound is $\exp(d_F(\text{Sep}))$, so the question is essentially equivalent to computing the facial dimension of $\text{Sep}(\mathbb{C}^d \otimes \mathbb{C}^d)$. Since its linear dimension is $d^4 - 1$, an upper bound of $O(d^4)$ follows from general arguments. Closing the gap between this upper bound and the lower estimate $\Omega(d^3 / \log d)$ seems an interesting question. While related constructions using nets were considered by various authors, it seems likely that having a new class of invariants to focus on may lead to sharper results.
- **More/less robust entanglement.** For which values of ε_d in Theorem 1' can we conclude that $N \gg 1$? Note that this question is meaningful only for $\varepsilon_d > \frac{2}{2+d^2}$ since any $\rho \in D(\mathbb{C}^d \otimes \mathbb{C}^d)$ has the property that $\frac{2}{2+d^2} \bullet \rho$ is separable [41]. In the opposite direction, the reader will notice that the assertions of Theorem 1 and Theorem 1' differ rather modestly, and that we do not get further strengthening if we let ε to be close to 1 (i.e., if we insist that the family of witnesses be universal for all ρ such that $(1 - \delta) \bullet \rho$ is entangled for some small $\delta > 0$, or even if we let $\delta = \delta_d \rightarrow 0$ when $d \rightarrow \infty$). This is because our lower bound on $d_F(\text{Sep}, A)$ does not improve substantially when $A \rightarrow 1$. However, it is still conceivable that, for some other general reasons, Sep is harder to “finely-approximate” by a polytope with few faces than D , which would perhaps allow to retrieve the results of [36] from general principles, and to link the perspective provided by our approach with the prior algorithmic results on entanglement detection.
- **Multipartite or unbalanced setting.** What if the underlying Hilbert space is of the form $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^m$ or $\mathcal{H} = (\mathbb{C}^d)^{\otimes N}$?
- **Unbalanced witnesses.** What if we use witnesses $\Phi : M_d \rightarrow M_m$, where $m = \text{poly}(d)$?

Finally, our primary motivation was to bring to the attention of the quantum information/theoretical computer science communities another tool from asymptotic geometric analysis, which didn't seem to be widely known. Given the strong algorithmic flavor of the (40 years old!) Figiel–Lindenstrauss–Milman inequality (6), it is quite likely that it has applications to complexity theory that go beyond entanglement detection.

REFERENCES

- [1] Guillaume Aubrun and Cécilia Lancien. Locally restricted measurements on a multipartite quantum system: data hiding is generic. *Quantum Inf. Comput.*, 15(5-6):513–540, 2015.
- [2] Guillaume Aubrun and Stanisław Szarek. *Alice and Bob meet Banach. The Interface of Asymptotic Geometric Analysis and Quantum Information Theory*. In preparation.
- [3] Guillaume Aubrun, Stanisław Szarek, and Elisabeth Werner. Hastings’s additivity counterexample via Dvoretzky’s theorem. *Comm. Math. Phys.*, 305(1):85–97, 2011.
- [4] Guillaume Aubrun and Stanisław J Szarek. Tensor products of convex sets and the volume of separable states on n qudits. *Physical Review A*, 73(2):022109, 2006.
- [5] Guillaume Aubrun, Stanisław J. Szarek, and Deping Ye. Phase transitions for random states and a semicircle law for the partial transpose. *Phys. Rev. A*, 85:030302, Mar 2012.
- [6] Guillaume Aubrun, Stanisław J. Szarek, and Deping Ye. Entanglement thresholds for random induced states. *Comm. Pure Appl. Math.*, 67(1):129–171, 2014.
- [7] Alexander Barvinok. Thrifty approximations of convex bodies by polytopes. *Int. Math. Res. Not.*, 2014(16):4341–4356, 2014.
- [8] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.
- [9] Fernando G.S.L. Brandão, Matthias Christandl, and Jon Yard. A quasipolynomial-time algorithm for the quantum separability problem. In *Proceedings of the 43rd annual ACM symposium on theory of computing, STOC ’11. San Jose, CA, USA, June 6–8, 2011.*, pages 343–352. New York, NY: Association for Computing Machinery (ACM), 2011.
- [10] E.M. Bronstein. Approximation of convex sets by polytopes. *Journal of Mathematical Sciences*, 153(6):727–762, 2008.
- [11] Aryeh Dvoretzky. Some results on convex bodies and Banach spaces. In *Proc. Internat. Sympos. Linear Spaces (Jerusalem, 1960)*, pages 123–160. Jerusalem Academic Press, Jerusalem; Pergamon, Oxford, 1961.
- [12] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.
- [13] T. Figiel, J. Lindenstrauss, and V. D. Milman. The dimension of almost spherical sections of convex bodies. *Acta Math.*, 139(1-2):53–94, 1977.
- [14] Sevag Gharibian. Strong NP-hardness of the quantum separability problem. *Quantum Inf. Comput.*, 10(3-4):343–360, 2010.
- [15] Y. Gordon. On Milman’s inequality and random subspaces which escape through a mesh in \mathbf{R}^n . In *Geometric aspects of functional analysis (1986/87)*, volume 1317 of *Lecture Notes in Math.*, pages 84–106. Springer, Berlin, 1988.
- [16] Leonid Gurvits. Classical deterministic complexity of Edmonds’ problem and quantum entanglement. In *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, pages 10–19. ACM, 2003.
- [17] Leonid Gurvits and Howard Barnum. Largest separable balls around the maximally mixed bipartite quantum state. *Physical Review A*, 66(6):062311, 2002.
- [18] Gus Gutoski, Patrick Hayden, Kevin Milner, and Mark M. Wilde. Quantum interactive proofs and the complexity of separability testing. *Theory Comput.*, 11:59–103, 2015.
- [19] Kil-Chan Ha and Seung-Hyeok Kye. Entanglement witnesses arising from exposed positive linear maps. *Open Syst. Inf. Dyn.*, 18(4):323–337, 2011.
- [20] Aram W. Harrow and Ashley Montanaro. Testing product states, quantum merlin-arthur games and tensor optimization. *J. ACM*, 60(1):3:1–3:43, February 2013.

- [21] Aram W. Harrow, Anand Natarajan, and Xiaodi Wu. Limitations of monogamy, Tsirelson-type bounds, and other semidefinite programs in quantum information. In preparation.
- [22] Matthew B Hastings. Superadditivity of communication capacity using entangled inputs. *Nature Physics*, 5(4):255–257, 2009.
- [23] W. Hoeffding. Probability inequalities for sums of bounded random variables. *J. Am. Stat. Assoc.*, 58:13–30, 1963.
- [24] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223(1–2):1–8, 1996.
- [25] Paweł Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Physics Letters A*, 232(5):333 – 339, 1997.
- [26] Lawrence M. Ioannou. Computational complexity of the quantum separability problem. *Quantum Inf. Comput.*, 7(4):335–370, 2007.
- [27] Paul Lévy. *Problèmes concrets d'analyse fonctionnelle. Avec un complément sur les fonctionnelles analytiques par F. Pellegrino*. Gauthier-Villars, Paris, 1951. 2d ed.
- [28] Alexander E. Litvak, Mark Rudelson, and Nicole Tomczak-Jaegermann. On approximation by projections of polytopes with few facets. *Israel Journal of Mathematics*, pages 1–20, 2014.
- [29] V. D. Milman. A new proof of A. Dvoretzky's theorem on cross-sections of convex bodies. *Funkcional. Anal. i Priložen.*, 5(4):28–37, 1971.
- [30] Asher Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413–1415, Aug 1996.
- [31] Gilles Pisier. *The volume of convex bodies and Banach space geometry*, volume 94 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1989.
- [32] C. A. Rogers. A note on coverings. *Mathematika*, 4:1–6, 1957.
- [33] C. A. Rogers. Covering a sphere with spheres. *Mathematika*, 10:157–164, 1963.
- [34] Gideon Schechtman. A remark concerning the dependence on ϵ in Dvoretzky's theorem. In *Geometric aspects of functional analysis (1987–88)*, volume 1376 of *Lecture Notes in Math.*, pages 274–277. Springer, Berlin, 1989.
- [35] E. Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31:555–563, 10 1935.
- [36] Łukasz Skowronek. How much is 2 different from 3? Entanglement detecting criteria in $N \times N$ systems. available at http://www.fizyka.umk.pl/zfmis/smp44/LNotes/Conference_talks/June_22/skowronek.pdf, 2012.
- [37] Erling Størmer. Positive linear maps of operator algebras. *Acta Math.*, 110:233–278, 1963.
- [38] Stanisław J. Szarek. Approximation by polytopes, coarse embeddings into ℓ_∞^n and rough nets of the Banach–Mazur compactum. 2014.
- [39] Stanisław J. Szarek, Elisabeth Werner, and Karol Życzkowski. Geometry of sets of quantum maps: a generic positive map acting on a high-dimensional system is not completely positive. *J. Math. Phys.*, 49(3):032113, 21, 2008.
- [40] Joel A Tropp. User-friendly tail bounds for sums of random matrices. *Foundations of Computational Mathematics*, 12(4):389–434, 2012.
- [41] Guifre Vidal and Rolf Tarrach. Robustness of entanglement. *Physical Review A*, 59(1):141, 1999.
- [42] Reinhard F. Werner. Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, Oct 1989.

INSTITUT CAMILLE JORDAN, UNIVERSITÉ CLAUDE BERNARD LYON 1, 69622 VILLEURBANNE CEDEX, FRANCE.

E-mail address: aubrun@math.univ-lyon1.fr

CASE WESTERN RESERVE UNIVERSITY, CLEVELAND, OHIO 44106-7058, USA.

INSTITUT DE MATHÉMATIQUES DE JUSSIEU-PRG, UNIVERSITÉ PIERRE ET MARIE CURIE, 75005
PARIS, FRANCE

E-mail address: `szarek@cwru.edu`